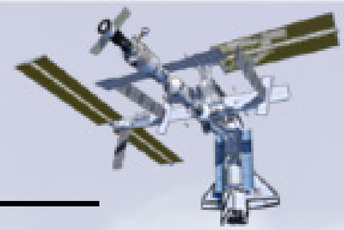
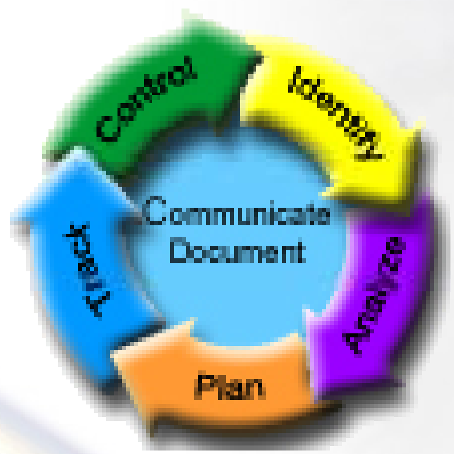


A Risk Manager's Perspective: Lessons Learned for Future Exploration Systems



John V. Turner, PhD

What Is A Risk Managers Perspective?

- NASA HQ defines general RM paradigms, processes, and tools in our policies such as: 8000.4 and 7120.5
- To some extent each program or project is unique – and implementation of NASA RM policies will be somewhat unique
- As the program evolves, implementation of these policies will evolve due to the different focus of each phase of the project lifecycle
- It is the Risk Manager or RMO responsibility to:
  - Give NASA policy legs
  - Train the program in how to do RM
  - Hold hands
  - Referee
  - Monitoring progress and making course corrections
  - Identify holes in decision making wrt specific risks
  - Manage / implement QRA to support risk informed decision making

Purpose

- To describe lessons learned regarding the application of Risk Management practices on:
  - Developmental programs
  - Operational programs

- Drawn from Shuttle Return to Flight, Shuttle Upgrades development, ISS, Oil and Gas, DoD, and other industries
  - Personal experience
  - Advice from greybeards
  - Research

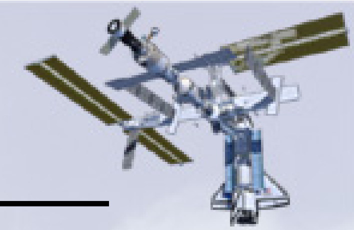
Topics For Discussion

- Shuttle RTF
- Space Shuttle Upgrades Development
- Developmental Risk Management

Shuttle Program RM Prior to STS-107

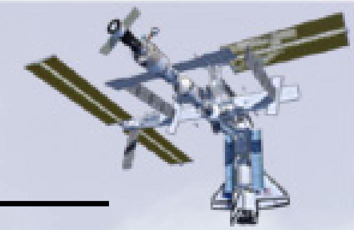
- SSP assumption prior to STS-107 was that the program team had a robust Risk Management process, a very mature understanding of our vehicle and our operational environment - adequate to prevent the occurrence of the STS 107 accident.
- During the RTF timeframe, both external and internal evaluations challenged these assumptions
- The CAIB noted many deficiencies in how the shuttle program managed risk indicting practice in almost all elements of RM
    - Identification, analysis, planning, tracking, control, communication, documentation

Shuttle Program RM: Prior to STS-107



- Lack of an ***integrated*** RM process influencing both tactical (next flight) and strategic (program life) decision making
- ***Segregation*** of "technical" (Safety and Mission Success) and "Programmatic" (Cost, Schedule, Supportability) risk
- Over reliance on ***qualitative*** HA and FMEA
- Over-reliance on the ***in-line safety*** organization to monitor program evolution and flag potential impacts to risk baseline
- Lack of a comprehensive or consistent system to examine implications of processing and flight ***anomalies*** to identify risk implications
- Lack of ***CRM process***
  - to tie various risk assessment activities together
  - To track progress
  - To establish risk reduction focus
- Lack of standard for the consideration of risk in ***major decisions***
- Development and Acquisition Strategy "locked in" risk due to design/organization/contracting approach - operational program management decisions exacerbated these risks through weak RM

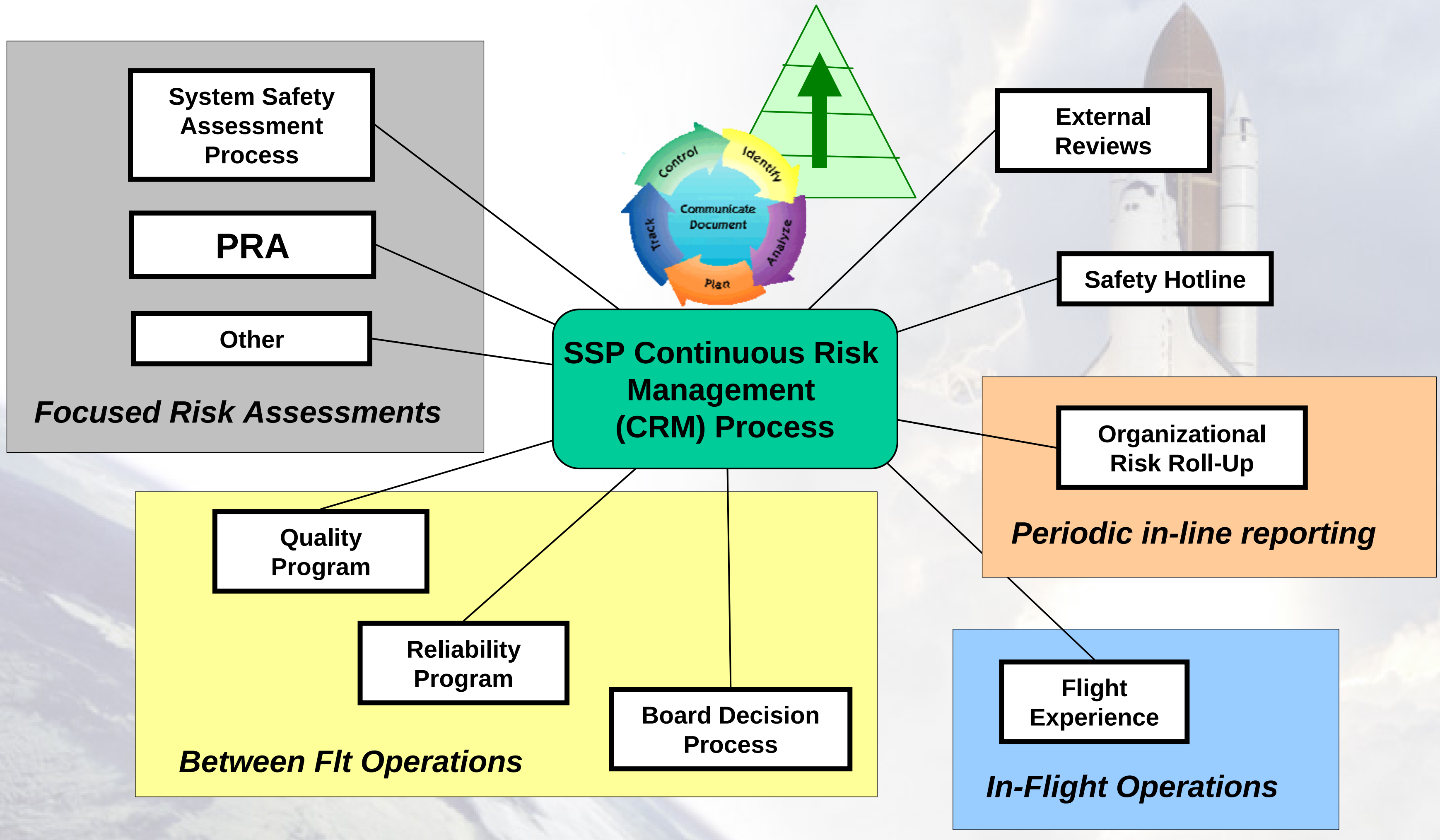
Shuttle Program RM: Recent Changes



- Developed and initiated independent SMA and ITA functions
- Major overhaul of SSP Hazard Analyses, waiver process
- Improved Commit-to-Flight Process
- Improved Mission Risk Management Capability
- Established CRM process, tools, and training
- Began integrating major risk related activities into the CRM process (Hazard Analysis, PRA risks, cost threats, non-conformances, etc.)
- Re-organized SPRA activities with central Technical Authority and budget
- Supported risk informed decision making with quantitative risk assessments
- Developed standard criteria for risk assessment to support major decisions
- Developed Safety Hotline System to provide an alternate (anonymous) path for risk reporting
- Developed updated integrated RM plan to include: pre-flight, commit-to-flight, and mission ops timeframes

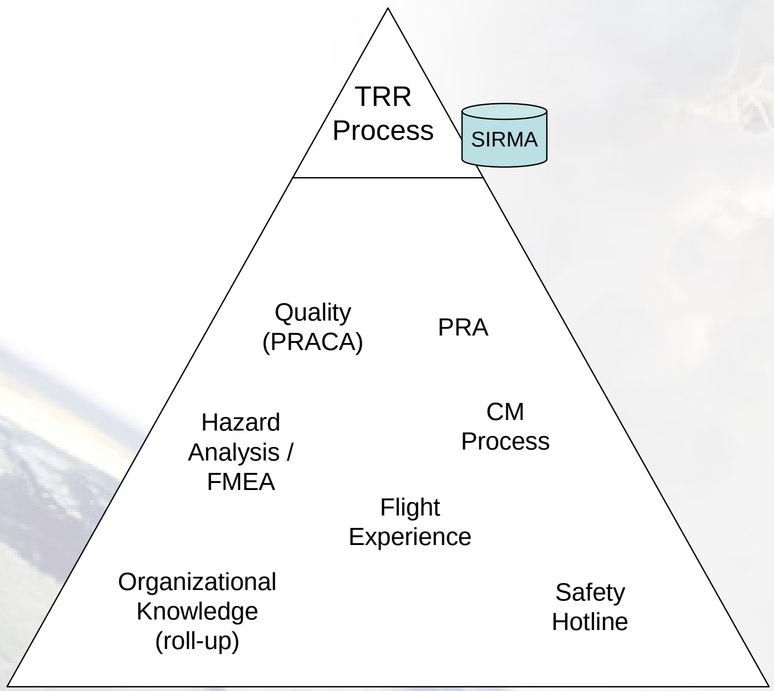
Significant Progress So Far, But Room For Improvement

Shuttle Program RM: Vision



Shuttle Program RM: Vision

- Risk Management integrates many sources of potential risk information into a hierarchical program risk communication process
- The extent to which this integration occurs will drive how accurate, complete and useful the CRM process is



Developmental Risk Management

"The beginning is the most important part of the work."

Plato

- Developmental program risk management should have a strong orientation to acquisition strategy, design, and project control
- Many developmental program RM lessons can be gleaned from shuttle operations, but shuttle upgrades, ISS development, other NASA developmental programs, and other industry development experience provides even more relevant experience

Development RM: Lessons Learned

- NASA RM policies are fairly high level (7120, 8000), limited in their scope, and do not encompass the whole lifecycle
  - Program / Project RM plans should define more detail wrt RM tools and practice (at an actionable level)
  - Leave room for tailoring in NASA policy
- Program/Project Manager is key to success
  - If the PM asks for risk assessment to support decisions, uses the risk management process to aggressively manage risks, and demands progress in risk mitigation – the RM process will work
  - Risk needs to be a part of real decision making processes
- Embed risk assessment and management program elements in the Systems Engineering template, instantiated in all project phases, and impacts all significant project functions, ex:
  - Risk should be a major consideration at ATP milestones
  - Requirements definition and management should be a risk informed process

Development RM: Lessons Learned

- The RM process is not just for the for the PM, or the program teams, or for headquarters – it is for all stakeholders
- A core RM team is critical to the development, care and feeding, of the RM process
  - Have enough resource to train, hold hands, participate in risk development when possible
- Establish training to introduce CRM, program unique risk processes, db tool
  - Any more than half a day will result in poor attendance
- RM is not just about a database, a 5x5 matrix, and communication processes. The bottom line is that we have to:
  - Perform proactive analysis to identify vulnerabilities and risks
  - Use this insight to influence the design process
  - Collaborate to resolve risks before they bite us
  - And then keep our models and processes alive to capture and manage future risks

Development RM: Lessons Learned

- The risk database is critical to communication and tracking, but better is often the enemy of good
  - Focus on most important features, most needed reports, ease of use: don't go crazy with "neat" functionality
  - *Let the process drive the database*
- Difficult to teach old dogs new tricks
  - Remember that more experienced NASA personnel may not have the same vision of RM that you do
  - Seek allies and be open to different ideas, but insist on effective practice
- The scorecard provides a rosetta stone for decoding risk communication
  - Goal based, need adequate level of detail, tailoring to project, but reflective of program priorities as well
  - Avoid Calculus with Crayons Syndrome (CWCS) – risk scores are at best fuzzy, if quantification is needed use QRA

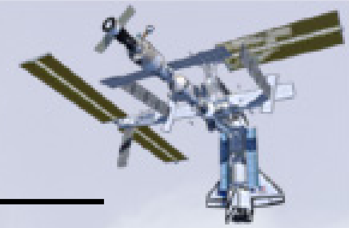
Lessons Learned

- Simplify Process and Beaurocracy As Much as Possible (Some Examples)
  - Three status codes
    - OPEN *(I am doing something about this)*
    - ACCEPTED *(I have decided not to do anything about this)*
    - CLOSED *(I significantly reduced to noise level)*
  - Two types
    - Concerns: *Not yet fully defined or accepted by owning team, invisible to all others but administrator*
    - Risks: *Concerns that have been escalated by owning team*
    - *Eliminated Watch Items and Cost Threats*
  - Often process improvements that really could add value in the mind of the developer are not worth the overhead
    - there is a point of diminishing returns where the more complicated this gets – the less likely it is to succeed

Lessons Learned

- RM is a Systems Engineering function
  - Vs SMA or Project Control
- Provide alternate venues for serious potential risks to be aired
- Structured Risk Identification through Taxonomies provide a better way to “brainstorm” risks
- Integration of project control systems is tough (complex and costly), but could pay large dividends
  - Decide up front if you are really going to make this a priority
- Identify risk drivers early: influence the acquisition plan, organizational structure, technology development approach, organization structure, staffing plan, etc.
  - Risk reduction capability diminishes over time, once the system is designed you have “locked in” risk
  - Get RM program requirements defined in contracts and subcontracts

Lessons Learned



- Problem Reporting and Corrective Action is a powerful surveillance tool for both development and operations
  - Integration, Consistency, Surveillance are essential
- Quantitative assessment should be an integral part of the design process - and becomes essential to operations and sustainment
  - System QRA, Focused Assessments, Quantified Hazards/FMEA
- QRA can encompass a broad range of methodologies, don't try to use a single approach (ex: complex linked fault-event tree) on all problems
  - Adapt methodology to the physics and available data
- Use QRA to draw conclusions and support decisions, not just to produce numbers
- Most managers think QRA is magic and distrust it
  - Ensure that you use a rigorous and defensible methodology and data set, answer all their questions, in most cases they will embrace it as a valuable tool
- Current NASA QRA Methodology is not well enough defined

Lessons Learned

- Establish a clear central technical authority for QRA to direct system QRA and adjudicate when conflicting PRAs arise
  - Budget for QRA and maintain a strong core capability
- Peer review is important, but: 1) select the right peer reviewers, 2) clarify scope for the review, 3) establish standards to review against
  - Peer review should be both internal and external
- PRA results can be very sensitive, treat them carefully
  - Whenever you talk the numbers – be sure the uncertainty and context is understood as well
  - Emphasize most significant contributors, action plans, scope, limitations, fidelity,
  - Several levels of documentation are needed
- Trading operations capabilities to simplify or economize during development is a perennial temptations to developers
  - Spares, Integrated Test, Reliability, performance, operating life, corrosion resistant paint, etc….

Lessons Learned

- Hardware / Software integration is tough!
- Integrated Cost and Schedule Risk Assessment is powerful
  - Bottoms up and top down
- SSUD Retrospective
  - Did not get started early enough on SSUD projects with RM
  - Did not have a core RM team
  - Several projects had significant technical challenges
  - Key RM requirements did not consistently flow down to the sub contracts
  - A lack of RM process and product surveillance led to surprises
  - Late requirements development
  - Early contractor down-select
  - SE template morphed from spiral – to sequential – to spiral waterfall (aka toilet)
  - Rationale for upgrades was, in some cases weak
  - Projects failed due to lack of funds and compelling rationale

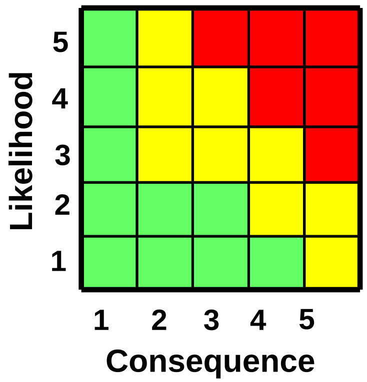
Summary

- NASA has the potential capability to make dramatic improvements in how risk is managed on exploration
- There is a distinct improvement in the attitudes of senior NASA management wrt the benefits of risk assessment and risk management
  - Take advantage of it
  - Bring them even further into the tent
  - Know your project, be engaged
  - Choose your battles
  - Be patient but insistent

BACKUP

SSP Risk Management Scorecard

Likelihood Rating	
5	**Very Likely: ~10^{-1}** Expected to happen in the life of the program.
4	**Likely: ~10^{-2}** Could happen in the life of the program. Controls have significant limitations or uncertainties.
3	**Possible: ~10^{-3}** Could happen in the life of the program. Controls exist, with some limitations or uncertainty.
2	**Unlikely**: ~10^{-4} Could happen in the life of the program, but not expected. Controls have minor limitations or uncertainties.
1	**Highly Unlikely: ~10^{-5}** Extremely remote possibility that it will happen in the life of the program. Strong controls in place.



Identify and Assess Risk

1. Start with a Concern. Is this a program risk?
   - What information is available? Gather information: requirements status, problem data, trends, hazards, critical item history, etc..
2. Define Risk Statement.
   - Given the condition _(A)_ , there is a possibility that _(B)_ will occur.
     - (A) - single phrase briefly describing current key circumstances, situations, etc. that are causing concern, doubt, anxiety, or uncertainty
     - (B) - Consequences, or impacts of the current conditions, that could be realized due to (A)
3. Define the Consequences (B). Locate the most accurate description(s) among the Safety, Mission Success, Supportability, Cost, and Schedule consequence descriptions.
4. How likely is this risk scenario? Locate the most accurate Likelihood Description that corresponds to the risk statement. Only one Likelihood Score is possible. Note: Quantitative likelihood ratings refer to program life, and are provided as guidelines only.
5. Plot the Risk. Select the highest consequence score. Plot this against the ONE Likelihood Score on the RED/YELLOW/GREEN risk matrix.

	Consequence Rating		1	2	3	4	5
TECHNICAL	**Safety**	*Human Health*	- Minor or First Aid Injury	- Moderate injury, illness, incapacitation or impairment	- Significant or long term, injury, illness, incapacitation or impairment	- Permanent or major injury, impairment, or incapacitation	- Death
		System Safety	- Damage to Non-Flight-Critical assets	- Loss of non flight critical assets	- Damage to major element(s) of flight vehicle or ground facility	- Loss major element(s) of flight vehicle or ground facility	- Loss of Program
		Evnronmental Safety	- Minor environmental Impact	- Moderate Envrionmental Impact	- Significant Environmental Impact	- Major Environmental Impact	- Catastrophic Environmental impact
		HSE Compliance	- Minor Non-Compliance	- Moderate Non-Compliance	- Significant Non-Compliance	- Major Non-Compliance	- Non Defined
	Mission Success	*Shutle Operations*	- Minor increase in flight operations timelines or complexity	- Failure to achieve any planned SSP mission objective	- Minimum Duration flight (MDF) - Significant increase in flight operations timelines or complexity	- Failure to achieve all Shuttle major mission objectives (MMO) - Early Mission Termination - Pad Abort or Intact Abort	- Contingency Abort
		ISS Operations	- None Defined	- Failure to achieve any planned ISS mission objective	- None Defined	- Failure to support assembly critical ISS requirements (*)	- Shuttle Crew Evacuation - ISS evacuation
		SSP Developmental Activities	- Failure to meet developmental requirements, Minor workarounds or temporary waivers required for flight	- None Defined	- Inability to complete Commit-to-Flight test, analysis or certification - Failure to meet developmental requirements. Significant or permanent waivers required for flight	- Failure to meet key development requirements (e.g. performance)	- None Defined
	Supportability	*Capability to Maintain SSP Assets*	- Temporary Usage Loss or LOCM of Non flight critical asset	- Permanent usage loss or LOCM of non-flight critical asset	- Temporary Usage Loss or LOCM, major element(s) of flight vehicle or ground facility	- Permanent usage loss or LOCM of major element(s) of flight vehicle or ground facility	- Inability to support further Shuttle Flight operations
		Flight Processing	- Collateral damage to non flight critical assets during processing	- Moderate increase timeline or complexity	- Significant increase timeline or complexity	- Collateral damage to major element(s) of flight vehicle or ground facility during processing	- None Defined
PROGRAMATIC	**Schedule**	*SSP / ISS Schedule*	- Minor Operational Slips,	- Less than 7 day slip in an SSP/ISS Freeze Point or milestone	- Greater than 7 day slip in an SSP/ISS Freeze Point or Milestone - ISS hardware/software delivery date not met for on-orbit needs	- 1 flight decrease from baselined manifest - 1 mission increase in ISS assembly plan - Flight delay occuring pre-FRR - SSP/ISS milestone slip of more than 1 month	- 2 or more flight decrease from baselined manifest - 2 or more mission increase in ISS assembly plan - Flight delay after L-2 - Cannot achieve major SSP/ISSP milestone
	Cost	*Risk Recovery Cost*	< \$1 M	\$1 M - \$10 M	\$10 M - \$40 M	\$40 M - \$70M	> \$ 70M